HU000022391 0B1

(19) **HU**

**MAGYAR KÖZTÁRSASÁG**
**Magyar Szabadalmi Hivatal**

(11) Lajstromszám: **223 910** (13) **B1**

# SZABADALMI LEÍRÁS

(21) A bejelentés ügyszáma: **P 01 02651**
(22) A bejelentés napja: **1998. 11. 23.**

(40) A közzététel napja: **2001. 12. 28.**
(45) A megadás meghirdetésének dátuma a Szabadalmi Közlöny és Védjegyértesítőben: **2005. 03. 29.**

(51) Int. Cl.[7]: **H 04 L 29/06**

(86) A nemzetközi (PCT) bejelentési szám:
**PCT/IB 98/01855**
(87) A nemzetközi közzétételi szám: **WO 0003525**

(30) Elsőbbségi adatok:
**98112938.0 1998. 07. 13. EP**

(72) Feltalálók:
**Hild, Stefan G., Adliswil (CH);**
**O'Connor, Luke J., Adliswil (CH)**

(73) Jogosult:
**International Business Machines Corp., Armonk, New York (US)**

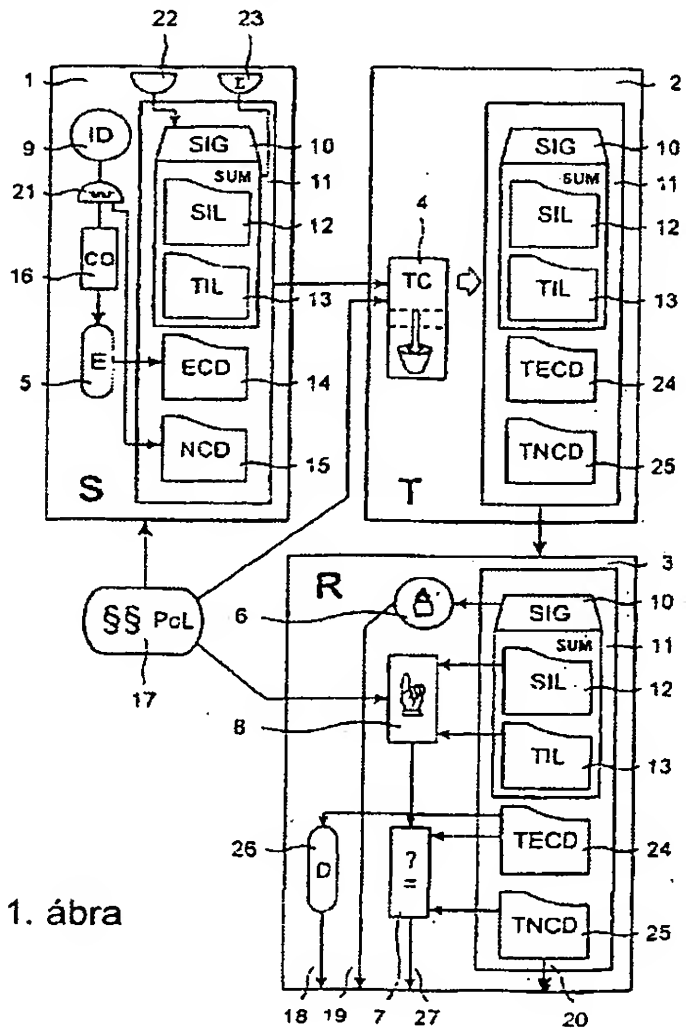
(74) Képviselő:
**Mák András, S. B. G. & K. Budapesti Nemzetközi Szabadalmi Iroda, Budapest**

(54) **Eljárás információadat továbbítására küldőtől fogadóhoz átkódolón keresztül, eljárás információadat átkódolására, eljárás átkódolt információadat fogadására, küldő, fogadó és átkódoló**

(57) Kivonat

A találmány tárgya egyrészt eljárás információadat (9) továbbítására küldőtől (1) fogadóhoz (3) átkódolón (2) keresztül, ahol az információadat (9) titkos információadatot (16) és nem titkos információadatot (15) tartalmaz. A találmány szerinti eljárásnál a titkos információadatot (16) kódolt titkos információadat (14) formára kódolják, amely a nem titkos információadattal (15) együtt képezi a részben kódolt információadatot (14, 15), és a részben kódolt információadattal (14, 15) együtt biztonsági információt (12) és átkódolásimód-információt (13) küldenek el az átkódolónak (2), a biztonsági információt (12) és az átkódolásimód-információt (13) az átkódolóval (2) egy átkódolási lépésben felhasználják, amelynek során a kódolt titkos információadat (14) tartalmához nem férnek hozzá, míg a nem titkos információadat (15) tartalmához az átkódolásnál hozzáférnek, tehát az átkódolóval (2) az átkódolási lépésben eldöntik, hogy a részben kódolt információadat (14, 15) mely részét továbbítják a fogadóhoz (3) és/vagy változtatják meg a továbbítás előtt.

A találmány tárgya másrészt eljárás részben kódolt információadat (14, 15) átkódolására átkódolóban (2), melyet küldőtől (1) kapnak meg, és fogadóhoz (3) kell továbbítaniuk. A találmány szerinti eljárásnál a részben kódolt információadat (14, 15) tartalmaz nem titkos információadatot (15) és kódolt titkos információadatot (14), és melyhez biztonsági információt (12) és átkódolásimód-információt (13) társítanak, melyet annak eldöntésére használnak, hogy a részben kódolt információadat (14, 15) mely részét kell átkódolniuk a fogadóhoz (3) történő továbbítás előtt, ahol a kódolt titkos információadatot (14) csak tartalmának felhasználása nélkül kódolják át, míg a nem titkos információadatot (15) a tartalom hozzáférésével kódolják át.




1. ábra





HU 223 910 B1

A találmány tárgya még eljárás átkódolt nem titkos információadatot (25) és átkódolt kódolt titkos információadatot (24) tartalmazó átkódolt részben kódolt információadat (24, 25) fogadására fogadónál (3) átkódolótól (2). A találmány szerinti eljárásnál az átkódolt részben kódolt információadattal (24, 25) együtt biztonsági információt (12) és átkódolásimód-információt (13) fogadnak, amelyeket az átkódolt részben kódolt információadattal (24, 25) való összehasonlításhoz használnak, az átkódolásnak a biztonsági információhoz (12) és átkódolásimód-információhoz (13) való megfelelésének tesztelésére.

A találmány tárgya ezenkívül az eljárást végrehajtó küldő vagy szerver (1), átkódoló (2) és fogadó vagy kliens (3).

---

A találmány küldőtől (szervertől) fogadóhoz (klienshez) átkódolón keresztül történő adatátviteli eljárással kapcsolatos, ami azt jelenti, hogy az információadatot megváltoztatjuk és/vagy redukáljuk a fogadóhoz történő átvitele előtt. A találmány tárgya továbbá eljárás az információadat átkódolására, különösképpen az információadat átkódolására akkor, amikor az egyaránt tartalmaz kódolt titkos információadatot és nem titkos információadatot. A találmány tárgya még eljárás az átkódolt információadat fogadására fogadónál történő átkódolással, különösképpen az információadat integritásának és az átkódoló megbízhatóságának ellenőrzésére. Ezenkívül a találmány tárgya küldő, átkódoló és fogadó, amelyek kombinálhatóak az átkódolás alatti információadat továbbításának végrehajtására.

Napjainkban az internetböngészés a világhálón (worldwide-web) nagymértékben stacionárius felhasználókra szorítkozik, akik hozzáféréssel rendelkeznek erőteljes számítási eszközökön, mint például munkaállomásokon vagy PC-ken futó böngészőkhöz. Ezen eszközök nemcsak viszonylag nagy sebességű és nagy sávszélességű adatkapcsolatokkal csatlakoznak az Internethez, hanem erőteljes szoftverrel és hardverrel vannak felszerelve a fogadott multimédiás adat feldolgozására és hozzáférhetővé tételére. A szerzők nagyban kihasználják ezt az infrastruktúrát olyan honlapok készítésével, melyek összetettsége egyre jobban nő, egyrészt az adattartalom tekintetében, amely nagyon változatos hang- és képformátumokat foglal magában, másrészt pedig a futtatható tartalom, mint a bővített funkciójú alkalmazások, úgymint fizetések stb. tekintetében.

Ahogy a felhasználók egyre jobban hozzászoknak ahhoz, hogy úgy támaszkodjanak a hálóra, mint általános célú információforrásra, úgy válik a hálóhoz való hozzáférés egyre kívánatosabbá mozgásban lévő felhasználók számára, akik olyan eszközöket használnak, mint mobiltelefon kézi készülékek vagy kicsi és könnyű kézi számítási eszközök. Mégis az ilyen eszközök használói problémákkal szembesülnek, amikor a világháló jelenlegi infrastruktúrájához próbálnak hozzáférni: a mobil kézi készülékek az Internethez túlságosan lassú és bizonytalan adatkapcsolattal csatlakoznak. Ez elfogadhatatlanul hosszú letöltési időkhöz vezet a nem hatékonyan formatált adatfolyamok esetében.

Ezen hordozható eszközök tartalomfeldolgozási kapacitása általában lényegesen kisebb, mint a PC-ké, mivel a rendelkezésre álló számítási teljesítmény korlátozott, és a letöltött tartalom megjelenítéséhez használt hardver nem elég fejlett. Például egy nagyon egyszerű mobil kézi készülék csak szöveges formátum ábrázolására képes.

Az Interneten lévő szerverek által kínált tartalmak közül sokat azzal a feltételezéssel hoztak létre, hogy az egy viszonylag erőteljes számítási eszközön kerül majd feldolgozásra és megjelenítésre. A szerver létre tudná hozni a tartalom több ábrázolását is, ahol minden egyes ábrázolás egy speciális számítási eszközre van szabva, mint például egy személyhívóra, egy mobiltelefon kézi készülékre, egy laptopra, egy nagyfelbontású PC-re, és így tovább. Mégis ez jelentős mennyiségű újraírást követel, mivel a szervertartalom nagy részét manuálisan kell módosítani. Minden egyes oldal több példányának karbantartása hasonlóképpen nemkívánatos.

A kliens számára egy alternatív megoldás egy átkódolási szolgáltatás használata. Egy átkódoló feladata egy szervertől kapott tartalom újraformázása annak érdekében, hogy a szerver és kliens közötti korlátozott sávszélesség ismeretében csökkentse a klienshez továbbítandó információ mennyiségét, és a kliens megjelenítési és feldolgozási képességének ismeretében biztosítsa, hogy így a továbbított adat ábrázolható a kliensnél. Ezért az átkódoló a kliens felőli adatkapcsolat ismeretét és a kliens feldolgozó/megjelenítő képességének ismeretét kívánja.

Az átkódoló által a kliensnek célzott tartalmon végezhető általános feladatok közé tartozik a hang- és grafikus tartalom eltávolítása, a grafikai formátumok közti konverzió, a tömörítés és kitömörítés, vagy egy jelöléses (marked-up) nyelvből, mint a HTML (Hypertext Marked-up Language), való konvertálás más adatábrázolásokba, például beszédre.

Általában a szervertől a kliensnek küldött minden tartalom áthalad az átkódolón. Az átkódolás végrehajtásához az átkódolónak korlátlan hozzáférésre van szüksége minden adathoz. Mivel az tartalmazhat biztonságérzékeny információt, az átkódolót megbízható félként kell kezelni. Ekkor a biztonság fenntartható egy biztonságos csatorna kiépítésével, például a biztonságos aljzatréteg (SSL – Secure-Socket-Layer)-protokollt használva a szerver és az átkódoló között, és egy különálló biztonságos csatorna kiépítésével az átkódoló és a kliens között, illetve az átkódoló beágyazásával vagy a szerverbe, vagy a kliensbe, és SSL használatával a kettő között. Ha az átkódoló nem megbízható, akkor az átkódolási szolgáltatás a kis értékű vagy értéktelen tartalmon végzendő műveletre korlátozódik.

Sajnos az átkódoló beágyazása a szerverbe vagy a kliensbe elfogadhatatlan néhány nagy biztonságérzékenységű alkalmazás kivételével, mivel az továbbfejlesztést igényel a szerverszoftver, és általában a szerverhardver tekintetében is. Ezenkívül a mobil eszközök gyors ütemben fejlődnek, és valószínűleg az átkódolók is hasonló ütemben fejlődnek, ami rövid szoftvercserélődési ciklusokhoz vezet.

Külső átkódolószolgáltatások, amelyeket kézikészülék-gyártók, egy adat-hálózatoperátor vagy egy Internet-szolgáltató (ISP – Internet Service Provider) kínálhatnak kereskedelmi szolgáltatásként, és amelyek egyesíthetőek létező proxy szerverekkel, egyértelműen alkalmazhatóbb és rugalmasabb megoldások. Sajnos az ilyen harmadik fél által biztosított átkódolókat ritkán tekinthetjük megbízható félnek. A biztonság ekkor az elejétől végéig való kódolással biztosítható a szerver és a kliens között, ami az átkódolót a kódolt adatfolyamon való működés lehetetlen feladata elé állítja.

A jelenlegi elejétől végéig való kódolási eljárásokkal együtt az ismert átkódolók nem használhatók, mivel ezek egyszerű szöveghozzáférést igényelnek az adatfolyam teljes egészére. Működésük nem ellenőrizhető a kliens által, amely még használhatatlanabbá teszi őket biztonságérzékeny adatátvitelek esetében.

Egy átkódolót ír le például az US 5,544,266 számú szabadalmi leírás. Az US 5,729,293 számú szabadalmi leírás egy például képek sorozatát ábrázoló kódolt digitális jeleket átkódoló eszközt ismertet, amely tartalmaz egy változtatható hosszúságú dekódolási csatornát, amelyet egy változtatható hosszúságú kódolási és dekódolási csatorna követ. Egy predikciós alegység van a két csatorna közé iktatva, és ez az alegység tartalmaz sorosan kötve két kivonó között egy képmemóriát és egy mozgáskompenzációs áramkört, amely az egyes képek mozgását kifejező eltolási vektorokkal dolgozik. Más megvalósítások is lehetségesek, amelyben a szóban forgó predikciós alegység tartalmaz legalább kettő, általában több hasonló kódoló- és dekódoló csatornát, melyek kaszkádba vannak kötve, és amelyek megfelelnek a képminőségszintek azonos számának.

Az US 5,745,701 számú szabadalmi leírás egy rendszert ismertet helyi hálózatok összekapcsolására nyilvános átviteli hálózaton keresztül, amelyben a helyi hálózathoz csatlakozó mikroszámítógép típusú egységek egy útválasztó (router) segítségével a nyilvános hálózathoz kapcsolhatók annak érdekében, hogy kommunikálhassanak egy vagy több mikroszámítógép típusú egységgel, amelyek legalább egy másik helyi hálózathoz vannak kapcsolva, és melyek képesek egy útválasztó (router) segítségével a nyilvános hálózathoz kapcsolódni. A rendszer tartalmazza a nyilvános hálózaton keresztül menő, helyi hálózatok közti kommunikációk kiépítésének biztonságvédelmét, amely egy hitelesítést cserélő (certificate exchange) mechanizmust és az aktív hitelesítéshez (active authentication) szükséges szoftvereljárásokat alkalmaz, amely „kérdés-válasz" („challenge-response") típusú, és az útválasztókban (router) helyezkedik el. A bemutatott hálózat egy tipikus felhasználási terület lenne az átkódolás használatára.

A találmány egyik célja olyan eljárás megadása információadat továbbítására küldőtől fogadóhoz átkódolón keresztül, amely lehetővé teszi nem megbízható átkódoló használatát információadat átkódolásra, amely ennek ellenére tartalmazhat kódolt titkos és nem titkos információadatot.

A kitűzött célt a találmány szerint egy olyan eljárással érjük el amelynek során a titkos információadatot kódolt titkos információadat formára kódoljuk, amely a nem titkos információadattal együtt képezi a részben kódolt információadatot, és a részben kódolt információadattal együtt biztonsági információt és átkódolásimód-információt küldünk el az átkódolónak, a biztonsági információt és az átkódolásimód-információt az átkódolóval egy átkódolási lépésben felhasználjuk, amelynek során a kódolt titkos információadat tartalmához nem férünk hozzá, míg a nem titkos információadat tartalmához az átkódolásnál hozzáférünk, tehát az átkódolóval az átkódolási lépésben eldöntjük, hogy a részben kódolt információadat mely részét továbbítjuk a fogadóhoz és/vagy változtatjuk meg a továbbítás előtt.

Az 1. igénypont szerinti jellemzőkkel bíró eljárás rendelkezik azzal az előnnyel, hogy bár titkos információadat kódolt formában kerül átkódolásra, az átkódolás elvégezhető úgy, hogy a nem titkos információadatot átkódoljuk, és a kódolt titkos információadat úgy kódolható át, hogy azt eltávolítjuk. Ily módon nincs szükség megbízható átkódolóra, sem további kommunikációs kapcsolatra a küldő és a fogadó között titkos információadat továbbítására.

Amikor a részben kódolt információadathoz ellenőrző (hashing) információt társítunk, amely a fogadónál lehetővé teszi a részben kódolt információadat legalább egy részének tartalom-ellenőrzését, egy további biztonsági mechanizmus alakul ki, amely ezáltal növeli az elérhető átviteli biztonságot, és minimalizálja a külső tisztességtelen szándékú behatásokat.

Előnyösnek bizonyul az, ha az információadatot további információadat-darabokra bontjuk fel kódolás és továbbítás előtt, mivel ezáltal pontosabb és finomabb felbontású információadat-kezelés érhető el, különösképpen annak paraméterei tekintetében. Egy ilyen paraméter a biztonság, amely azt mondja meg, hogy egy információadat-darab titkos-e vagy sem. Egy másik ilyen paraméter az átkódolási mód, amely azt mondja meg, hogy milyen átkódolási sajátosságok alkalmazhatóak a vonatkozó információadathoz. Ilyen sajátosságok lehetnek például, hogy az információadat-darab tömöríthető-e, vagy sem, hogy figyelmen kívül hagyható-e, vagy sem, és így tovább.

A fenti előny fokozható, ha minden egyes információadat-darabhoz hozzárendeljük a saját darab biztonságiinformáció-részét és darab átkódolásimód-információrészét úgy, hogy az információadat-darabok megkapják a saját hozzárendelt profiljukat, de legalább a biztonsági és átkódolásimód-információt. Ekkor az átkódoló egyenként kezelheti az információadatot, a hoz-

zá tartozó profilja szerint. Ekkor az információadat-darabok közötti függőségeket kiküszöböljük.

Ha egy információadat-darabhoz hozzárendeljük a saját darab ellenőrző- (hashing) információ-részét, amely információadat-darab lehetőség szerint része a nem titkos információadatnak, egy még finomabb felbontás érhető el a biztonságban. Mivel az ellenőrzésből (hashing) következik, hogy vonatkozó információadat tartalma nem változtatható meg, csak egy korlátozott átkódolási mód alkalmazható, nevezetesen semmilyen átkódolás vagy törlés. Ezért előnyösnek bizonyul, ha ezen ellenőrzés (hashing) olyan információadatokra korlátozódik, amelyek esetében arra valóban szükség van úgy, hogy maximális átkódolási szint legyen elérhető.

A darab biztonságiinformáció-részeket és darab átkódolásimód-információrészeket címkékre fordíthatjuk át átfordítási eljárás szerint, és a darab biztonságiinformáció-részek és darab átkódolásimód-információrészek helyett a címkéket továbbítjuk az átkódolóhoz, ahol az eljárásinformációt, mely megadja, hogy a címkéket hogyan kell értelmezni, elérhetővé tesszük, vagy már eleve elérhető az átkódoló számára. Az eljárás csökkenti az elküldendő információ mennyiségét. Ez különösen akkor igaz, amikor nagyszámú darab biztonságiinformáció-részt és darab átkódolásimód-információrészt kell továbbítanunk, mert az elért adatmegtakarítás a rövidebb címkék használatával egyre dominánsabbá válik az eljárásinformáció által hozzáadódó adattal szemben. Ezen eljárás hasonló rövid azonosítók, mint például betűszavak (acronym) használatához hosszan leírható műveletek helyett. Az eljárásinformáció ekkor megmondja, hogy milyen jelentés rejlik az azonosító vagy betűszó mögött.

A címkéket ezután kombinálhatjuk egy biztonsági és átkódolásimód-információcsomagban, melyet egy aláírással egészítünk ki, amely tartalomintegritás-ellenőrzést tesz lehetővé a fogadónál. Ennek az az előnye, hogy a fogadó meggyőződhet arról, hogy a biztonsági és átkódolásimód-információcsomag módosult-e, vagy sem. Ha a biztonsági és átkódolásimód-információcsomag nem módosult, leellenőrizheti, hogy a kapott információadat a biztonsági és átkódolásimód-információcsomagban foglalt szabályok szerint került-e átkódolásra. Máskülönben tudja, hogy az átkódoló hibásan működött, és a kapott információadat nem megbízható.

A találmány másik célja eljárás biztosítása részben kódolt információadat biztonságos átkódolására átkódolóban, ily módon csak a nem titkos információadat tartalmához való hozzáféréssel.

Ezt a célt a találmány szerint olyan eljárással érjük el, amelynél a részben kódolt információadat tartalmaz nem titkos információadatot és kódolt titkos információadatot, és amelyhez biztonsági információt és átkódolásimód-információt társítunk, melyet annak eldöntésére használunk, hogy a részben kódolt információadat mely részét kell átkódolnunk a fogadóhoz történő továbbítás előtt, ahol a kódolt titkos információadatot csak tartalmának felhasználása nélkül kódoljuk át, míg a nem titkos információadatot a tartalom hozzáférésével kódoljuk át.

Ezen eljárás a 8. igénypont szerinti jellemzőkkel előnyösen lehetővé teszi a fogadott információadat átkódolását a megbízhatóság szükségessége nélkül. Ehhez biztonsági információt és átkódolásimód-információt használunk, melyek megmondják az átkódolónak, hogy hogyan kell kezelnie a beérkező információadatot, nevezetesen hogy melyik információadat kódolt és melyik nem, és hogy milyen átkódolási eljárást kell követnie.

A találmány további célja olyan eljárás biztosítása az átkódolt információadat fogadására a fogadónál, ami által az átkódolónak a biztonsági feltételekkel és átkódolási feltételekkel szembeni megfelelése tesztelhető.

Ezt a célt a találmány szerint olyan eljárással érjük el, amelynek során az átkódolt részben kódolt információadattal együtt biztonsági információt és átkódolásimód-információt is fogadunk, amelyeket az átkódolt részben kódolt információadattal való összehasonlításhoz használunk, az átkódolásnak a biztonsági információhoz és átkódolásimód-információhoz való megfelelésének tesztelésére.

Az eljárás a 13. igénypont szerinti jellemzőkkel azon előnnyel rendelkezik, hogy az átkódoló megbízhatósági teszt nagyon egyszerű, és ugyanazon információra támaszkodik, melyet az átkódoló az átkódolásra használt. Mivel a biztonsági és az átkódolásimód-információ nem keveredik az információadattal, a biztonsági és átkódolásimód-információ integritás-ellenőrzése leegyszerűsödik, mert nincsen szükség átkódolásra, és így a biztonsági és átkódolásimód-információt megváltoztató hozzáférésre sem.

A címkék használata a biztonsági és átkódolásimód-információ rövidített verziójaként különösen hasznos akkor, amikor az ehhez használt átfordítási eljárás, amelyre a címkék értelmezésekor is szükség van, széles körben használt és esetleg szabványosított. Ekkor az eljárásinformáció átvitele az információadattal együtt nem szükséges, mert az már jelen van az átkódolóban, illetve ott a vonatkozó címkék automatikusan értelmezhetők, mert az átkódoló már megvalósította a címkéknek megfelelő funkcionalitást. Ekkor az átfordítási eljárást megvalósíthatjuk az átkódolóban közvetlenül a vonatkozó funkcionalitásban, ily módon elkerülve a konkrét értelmezés lépését. Például, amikor egy „NT" címke érkezik, az átkódoló automatikusan nem hajthatna végre átkódolást, mivel az átkódolót úgy programoztuk vagy határoztuk meg, hogy ilyen címkével rendelkező információadatot oly módon kezeljen, hogy nem végez rajta semmilyen átkódolást. A megfelelő átfordítás így „NT"=nincs átkódolás (no transcoding) lenne.

A biztonsági és átkódolásimód-információcsomag minden olyan információt megad, amelyre az átkódolónak szüksége van a beérkező információadat helyes feldolgozásához. Mivel a biztonsági és átkódolásimód-információ nem átkódolandó, ez a biztonsági és átkódolásimód-információcsomag kiegészíthető egy alá-

írással, lehetővé téve az ellenőrzést a fogadónál, hogy a biztonsági és átkódolásimód-információcsomag tartalma módosult-e valahol a küldő és a fogadó között. A biztonsági és átkódolásimód-információcsomag tisztességtelen szándékú vagy hiba jellegű módosítása így könnyen felismerhető a fogadónál, ami a teljes információadat-átvitelt biztonságosabbá teszi.

A találmány további célja küldő biztosítása adatátvitelre egy fogadóhoz átkódolón keresztül, amely lehetővé teszi egy nem megbízható átkódoló használatát információadat átkódolására, amely ennek ellenére tartalmazhat kódolt titkos és nem titkos információadatot.

Ezt a célt a találmány szerint olyan küldő kialakításával érjük el, amely tartalmaz kódolót a titkos információadat kódolására, előállító eszközt biztonsági információ és átkódolásimód-információ előállítására, valamint csatolóeszközt, amely a biztonsági információt és az átkódolásimód-információt a részben kódolt információadathoz csatolja az átkódolónak való továbbítás előtt, ahol a biztonsági információ és átkódolásimód-információ megakadályozza a hozzáférést a titkos adatokhoz, és lehetővé teszi a hozzáférést a nem titkos adatokhoz az átkódolás során.

A 19. igénypont szerinti jellemzőkkel bíró küldő azzal az előnnyel rendelkezik, hogy bár csak egyszerű módosítására van szükség az ismert küldőkhöz képest, az átkódolás előnyeit kombinálhatjuk a biztonságérzékeny, például titkos információadat biztonságos átvitelének előnyeivel.

Egy darabolóeszköz megvalósítása az információadat-kódolás és -továbbítás előtti, információadat-darabokra való további felosztására viszonylag egyszerű. Szövegszintaxist vagy képadatfejrész- (header) információt használhatunk automatikus felosztás elvégzésére.

A találmány célja még átkódoló biztosítása részben kódolt információadat biztonságos átkódolására, ily módon csak a nem titkos információadat tartalmához való hozzáféréssel.

Ezt a célt a találmány szerint olyan átkódolóval érjük el, amely tartalmaz döntési eszközt annak eldöntésére, hogy a fogadott részben kódolt információadat mely részét kell átkódolni a fogadóhoz való továbbítása előtt, ahol a kódolt titkos információadat csak a tartalmának felhasználása nélkül kódolható át, míg a nem titkos információadat átkódolható annak tartalmához való hozzáféréssel is.

A 23. igénypont szerinti jellemzőkkel bíró átkódoló azzal az előnnyel rendelkezik, hogy megfelelően kezeli a kódolt és nem kódolt információadatot tartalmazó információadatokat, és oly módon végezheti el a lehetséges optimális átkódolást, hogy nem próbál hozzáférni a kódolt információadat tartalmához, viszont hozzáfér a nem titkos információadathoz az átkódolás érdekében. Minél mélyebbre képes az átkódoló ásni az információadatban, annál nagyobb lehet az átkódolási hatékonyság az átkódolóban lévő pontosabb ismeret következtében arról, hogy melyik információt milyen mértékben csökkenthetjük. Mégis, kódolt információadat nem hozzáférhető ilyen tartalomvizsgálathoz a küldő szándéka szerint. A szükséges információ ahhoz, hogy az információadat mely részét hogyan kezeljük származtatható a biztonsági és átkódolásimód-információból.

A találmány célja ezenkívül fogadó biztosítása az átkódolt információadat fogadására a fogadónál, ahol az átkódoló megfelelése a biztonsági feltételek és átkódolási feltételek tekintetében tesztelhető.

Ezt a célt a találmány szerint olyan fogadó kialakításával érjük el, amely tartalmaz összehasonlító eszközt a biztonsági információnak és az átkódolásimód-információnak az átkódolt részben kódolt információadathoz való hasonlítására az átkódolásnak a biztonsági információhoz és átkódolásimód-információhoz való megfelelésének tesztelésére.

A 25. igénypont szerinti jellemzőkkel bíró fogadó rendelkezik azzal az előnnyel, hogy az átkódolási technika összes előnyét élvezi anélkül, hogy szükség lenne megbízható átkódolóra vagy különálló titkos információ-kommunikációsvonallal rendelkezni a küldőhöz. A küldőtől a fogadóhoz való úton az információadat bármely nem engedélyezett módosítása könnyen felismerhető a biztonsági és átkódolásimód-információ használatával, amely önmagában védett a rejtett módosításokkal szemben. Észrevétlen információmeghamisítás így nem lehetséges, illetve rögtön semlegesítődik kódolási technológia használatával, mely a használt kódolási algoritmustól függően nagyon nagy biztonságot nyújt.

A megoldott probléma a két végpont közti biztonságos kommunikáció könnyebbé tétele egy fogadó, például egy kliens, és egy küldő, például egy szerver között, miközben engedélyeznek egy közbülső átkódolási szolgáltatást a tartalom megváltoztatására a kliens képességei és összekapcsolhatósági tulajdonságai szerint. A javasolt megoldás olyan szerverből indul ki, amelynek a tartalmát két információadat-típusra lehet osztani. Ezek egyikének védettnek kell lennie a titkosság végett, a másik pedig nem titkos vagy esetleg akár nyilvános, és átkódolható. Ezen megközelítés két célt elégít ki:

- Lehetővé teszi átkódolási technikák alkalmazását biztonságérzékeny adatot tartalmazó adatfolyamon magához a biztonságérzékeny adathoz való egyszerű szöveges hozzáférés megkövetelése nélkül, és az átkódoló által elvégzett átkódolás a kliens által ellenőrizhető.
- Az eljárás lehetővé teszi nem megbízható átkódolószolgáltatás működését biztonsági vonatkozású adatfolyamon anélkül, hogy az adatfolyamban lévő biztonságérzékeny adatelemek elejétől végéig való kódolásával kompromisszum születne.

Az információadat tovább osztható mezők együttesére, melyek vagy titkos, vagy nem titkos típusúak.

Ezenfelül a rendszer rugalmas abból a szempontból, hogy az egyes adatmezők átkódolhatóságát és titkosságát a kívánt biztonság érdekében a szerver határozhatja meg.

Továbbá az átkódoló által végzett műveletek ellenőrizhetőek olyan vonatkozásban, hogy az átkódoló csak az elfogadott eljárás szerint módosította a tartal-

mat. Itt azon feltételezéssel élünk, hogy a tartalom biztonságos (titkos) mezői nem kívánnak átkódolást.

A megoldás alkalmazható olyan elrendezéseknél, ahol elektronikus kereskedelmi, on-line banki vagy más biztonságérzékeny alkalmazások futnak korlátozott beviteli vagy kiviteli lehetőségekkel, és a szerverhez való korlátozott sávszélességű kapcsolatokkal rendelkező Tier-0 vagy Tier-1 klienseken anélkül, hogy megkövetelnénk a szerverektől, hogy installáljanak és futtassanak egy kitüntetett és megbízható átkódolási funkciót, vagy ahol új és javított eszközlehetőségek, így átkódolási funkciók gyors fejlődési ciklusaira számítunk, és ahol így független átkódolószolgáltatásokat preferálunk.

Kiindulva egy kezdeti, adatmezőkre vagy információadat-darabokra osztott információadat-folyamból, a javasolt eljárás a következő lépésekből állhat:

- További jelzők (tag), illetve címkék, beszúrása az eredeti adatfolyamba, amelyek az adat mezőket jelölik azok átkódolhatóságával, pl.: átkódolható, nem átkódolható, opcionális, kritikus stb., és biztonsági vonatkozásaival, pl.: biztonságérzékeny, biztonságra nem érzékeny stb., mely címkékre a továbbiakban úgy utalunk, mint biztonsági címkék vagy darab biztonságiinformáció-rész címke és darab átkódolásimód-információrész címkék.
- Eljárás (policy) dokumentum generálása, mely definiálja az átkódoló számára engedélyezett műveleteket minden egyes jelzőnél (tag). Ez az eljárásdokumentum vagy eljárásinformáció tartalmazza az egyes címkék jelentését, illetve azt, hogy hogyan kell azokat értelmezni. Ezt a lépést kihagyhatjuk, ha az átkódolón belül az eljárás kezdettől fogva ismert.
- A biztonságérzékeny információmezők elkülönítése, és elejétől végéig való kódolás alkalmazása rájuk választottan és egyedenként, a biztonságra nem érzékeny információmezőket kódolatlanul hagyva.
- Dokumentumösszegzés, másként biztonsági és átkódolásimód-információcsomag generálása az eredeti bemeneti folyam struktúrája alapján, tehát a biztonsági címkék és átkódolásimód-címkék beillesztése.
- A fogadó, pl.: kliens számára az átkódolóműveletek ellenőrzésének lehetővé tétele az átkódoló kimenetének összehasonlításával a dokumentumösszegzéssel és az eljárásdokumentummal.

A találmányt a továbbiakban a mellékelt rajzon példaképpen bemutatott kiviteli alak alapján ismertetjük részletesebben, ahol az

1. ábra egy küldőt, átkódolót és fogadót tartalmazó rendszer vázlata.

Az ábrát az érthetőség érdekében nem valós méretekben mutatjuk, és az egyes méretek közti kapcsolatok sem valós nagyságrendben láthatók.

Az 1. ábrán 1 küldő (másként szerver) 2 átkódolón keresztül 3 fogadóhoz (másként klienshez) csatlakozik egy kommunikációs kapcsolaton keresztül, amelynek nem kell fizikai kapcsolatnak lennie. Az 1 küldő, a 2 átkódoló, és a 3 fogadó egyaránt hozzáfér 17 eljárásinformációhoz.

Az 1 küldő tartalmaz 21 felbontóeszközt ID-vel jelölt (ID – information data), a 3 fogadóhoz küldendő 9 információadat további felosztására. A 21 felbontóeszköz kimenetén CD-vel jelölt (CD-confidential data) 16 titkos információadat és nem titkos 15 információadat, rövidítve NCD (NCD – nonconfidential data) jelenik meg. A 16 titkos információadat kódolására 5 kódolót (E – encoder) alkalmazunk, mely ECD-vel jelölt (ECD – encrypted confidential data) kódolt titkos 14 információadatot szolgáltat. Ezenkívül az 1 küldő 23 csomagosítót (packetizer) és 22 aláírás-generátort is tartalmaz.

A 9 információadatra ebben az esetben D tartalomként hivatkozunk, amely felbontható N darab $f_1$, $f_2$...$f_n$ tartalommező, vagy információadat-darab összességére. Itt egy mező ábrázolhat például egy szövegbekezdést, egy képet vagy táblázatba rendezett adatokat. További lehetséges eset, hogy az adott $f_1$ mező több $f_{i,1}$, $f_{i,2}$...$f_{i,n}$ almezőből áll, arra a tényre utalva, hogy a tartalom hierarchikus. Például, egy $f_1$ bekezdésmező állhat egy szövegmezőből, amelyet egy táblázatmező követ, amelyet egy képmező követ, és aztán további szövegmezők következnek. Az almezők is tartalmazhatnak további almezőket és így tovább. A mezőfelbontás részletessége a szerver kívánsága szerinti. A felbontást 21 felbontóeszközzel érjük el, amely itt a mezőket a kívánt biztonság szerint is szétválogatja.

Miután a mezőfelbontást elvégeztük, az 1 küldő minden egyes $f_1$ mezőhöz hozzáfűz vagy hozzárendel két osztályba sorolható címkéket. Az első címkeosztály az $L_S$ biztonsági címke, másként darab biztonságiinformáció-rész, mely jelzi, hogy az adott $f_i$ mező kódolandó-e az átvitel idejére. Például, a lehetséges $L_S$ biztonsági címkék halmazát definiálhatnánk úgy, mint

$$L_S=\{\text{biztonságos, nem biztonságos}\} \quad (1)$$

és $L_S(f_i) \in L_S$, ahol $L_S(f_i)$ az $f_i$ mező biztonsági címkéje. Az $L_S$ biztonsági címkét kiterjeszthetjük sokféle módon, például úgy, hogy tartalmazzon kódolási szinteket például rövid vagy hosszú kulcsokkal, tartalmazzon eredetiséginformációt vagy tartalmazzon aláírást.

A második címkeosztály egy $L_t$ átkódolási címke, vagy darab átkódolásimód-információrész, mely jelzi, hogy a 2 átkódoló milyen műveletet hajthat végre, amikor egy tartalommező érkezik. Például az $L_t$ átkódolási címkék egy lehetséges halmazát definiálhatnánk úgy, mint

$$L_t=\{\text{nem átkódolható, átkódolható, kritikus, nem kritikus}\} \quad (2)$$

ahol ezen címkék pontos jelentését 1 küldőhöz kapcsolódó átkódolási eljárásban definiálhatnánk. Például egy ilyen eljárás lehetne az $L_t$ átkódolási címkék következő értelmezése:

„átkódolható" arra utal, hogy a tartalommező átkódolható a 2 átkódoló kívánsága szerint;

„nem átkódolható" arra utal, hogy 2 átkódoló ne változtassa meg az 1 küldőtől (szervertől) kapott tartalommezőt;

„kritikus" arra utal, hogy a mezőt továbbítani kell a kérelmező 3 fogadónak (kliensnek) 2 átkódolótól;

„nem kritikus" arra utal, hogy 2 átkódoló törölheti a tartalommezőt a kérelmező 3 fogadóhoz továbbított tartalomból.

Az 1 küldő kiadhat egy pol(S) eljárásközleményt, amely $L_S(S)$ biztonsági címkék és $L_t(S)$ átkódolási címkék halmazát tartalmazza, és egy közleményt arról, hogy a címkéket hogyan kell értelmezni. Mivel a pol(S) eljárásközlemény nem tartalmaz biztonságérzékeny információt, bármikor lekérhető 1 küldőtől, és eltárolható későbbi felhasználás céljából egy az 1 küldőhöz való kapcsolódáskor a tartalomlekérés érdekében.

Itt feltesszük azt, hogy az átfordítási eljárást úgy választottuk, hogy az követi a már ismert és 2 átkódoló számára hozzáférhető 17 eljárásinformáció szabályait. Így itt nincsen szükség pol(S) eljárásközlemény kiadására. Az ismert 17 eljárásinformáció lehet például egy széles körben használt eljárás, egyfajta szabvány, amely ezáltal ismert lehet sok átkódoló, küldő és fogadó számára úgy, hogy a 17 eljárásinformáció létrehozása és elfogadása nem szükséges küldő számára.

A D tartalom adott $f_1, f_2 \ldots f_N$ mezőre történő felbontása mellett az 1 küldő kódol minden egyes $f_i$ mezőt, egy mezőcímkesorban (tuple), mint

$$L(f_i)=<L_S(f_i),L_t(f_i),[H(f_i)]> \quad (3)$$

ahol $L_S(f_i)$ $f_i$ mező biztonsági címkéje és $L_t(f_i)$ $f_i$ mező átkódolási címkéje, és H(...) egy kriptográfiai ellenőrző (hashing) függvény, másként ellenőrző (hashing) információ vagy hash, mint például az SHA–1 algoritmus. A $H(f_i)$ ellenőrző (hashing) függvényre, mely alkalmazható az $f_i$ mezők nulla, egy vagy több mezőjére, úgy is hivatkozunk, mint az információadatdarab-ellenőrző (hashing) információ részére, és szögletes zárójelben $[H(f_i)]$-ként specifikáljuk annak jelölésére, hogy ez opcionális mező. Amint azt a későbbiekben alább leírjuk, egy mező ellenőrző információját (hash-ét) magában foglalja az ő mezőcímkesora (tuple), ha a mező tartalmai ellenőrizendők a kérelmező 3 fogadó által, abban az értelemben, hogy a mezőadatot kódolatlanul küldjük el átkódolás végzése nélkül.

Az $L_S$ $(f_i)$ biztonsági címkék és $L_t(f_i)$ átkódolási címkék általánosságban $L_S$-ből és $L_t$-ből származó értékek egy listájából állhatnak. Például (2) képlet szerint definiált $L_t$ használatával az $f_i$ mező átkódolási címkéje lehetne

$$L_t(f_i)=\{\text{átkódolható, nem kritikus}\} \quad (4)$$

abban az értelemben, hogy a 2 átkódoló választhat, hogy elküldje-e $f_i$ mező egy ábrázolását a kérelmező 3 fogadónak, és ezenkívül a 2 átkódoló kiválaszthatja ezt az ábrázolást. Egy $f_{i,1}, f_{i,2} \ldots f_{i,ni}$ almezőkkel rendelkező $f_i$ mező számára a (2) képletbeli kódolási sémát rekurzívan alkalmazva kapjuk, hogy

$$L(f_i)=<L_S(f_i),L_t(f_i),L(f_{i,1}),L(f_{i,2})\ldots L(f_{i,ni}), [H(f_i)]> \quad (5)$$

és ha $H(f_i)$-re szükség van, ezt a mezőre és annak összes almezőjére kiszámítjuk.

A címkézés elvégezhető valamely címkézőeszközzel, amelybe betáplálhatjuk a szükséges információt ahhoz, hogy tudjuk, hogy a 9 információadat mely részét kell kódolnunk, és mely része lehet tárgya milyen módú átkódolásnak. Így a címkézőeszköz bementi adatként használja a 21 felbontóeszközből kijövő információadat-darabokat. A címkék sorrendjét így az információadat-darabok sorrendje szerint választjuk, hogy könnyebbé tegyük a címkék későbbi hozzárendelését a megfelelő információadat-darabhoz, nevezetesen a 2 átkódolóban és a 3 fogadóban. A címkézőeszközbe vagy címkézőbe táplálhatunk felhasználói preferenciákat, hogy információt adjunk a címkézőnek arról, hogy mely információadat-darabot kell kódolni és/vagy átkódolni és hogyan. Tehát a címkézés függhet valamely automatikus rendszertől, amely automatikusan hozzárendeli a vonatkozó címkéket például valamely megvalósított szabályokat követve, és/vagy függhet adott szabályoktól vagy egyéni címkézési preferenciáktól, melyeket a felhasználó ad meg vagy egy listáról származnak. Néha a címkézés elvégezhető egy rögzített sémát követve, és néha egy személyre szabott címkézési lista lehet az optimális megoldás ahhoz, hogy megmondjuk a címkézőnek, hogy melyik címkeértéket kell hozzárendelni melyik adatdarabhoz.

A rajzon a biztonsági címkék összességének csoportjára úgy hivatkozunk, mint a darab biztonságiinformáció-részek csoportja, melyet SIL–lel jelölünk (SIL – security information label), míg az átkódolási címkék csoportjára úgy hivatkozunk, mint a darab átkódolásimód-információrészek csoportja, melyet TIL–lel jelölünk (TIL – transcoding-type information label). Más szavakkal, minden egyes mezőnek, az információadat-darab tekintetében, van saját darab biztonságiinformáció-része, amelynél az összes darab biztonságiinformáció-rész együtt adja a biztonsági információt. A biztonsági információt felbonthatjuk az összes biztonsági címke csoportjára és a megfelelő átfordításieljárás-információra. Így minden egyes mezőre a darab biztonságiinformáció-részt is felbonthatjuk a biztonsági címkére és a megfelelő átfordításieljárás-információra, röviden eljárásinformációra.

A TIL a megfelelő eljárásinformációval együtt adja a 13 átkódolásimód-információt, melyet az ábrán egyszerűsített formában ábrázolunk. A SIL a megfelelő eljárásinformációval együtt adja a 12 biztonsági információt, amelyet az ábrán szintén egyszerűsített formában ábrázolunk. Az elv az, hogy a 2 átkódoló számára biztosítani kell az 1 küldő akarata szerinti átkódolás végrehajtásához szükséges információt, amely olyan formában van kifejezve, amit a 2 átkódoló megérthet és értelmezhet a helyes végrehajtás érdekében. Ez azt jelenti, hogy a 12 biztonsági információt és a 13 átkódolásimód-információt továbbítjuk a 2 átkódolóhoz, vagy a címke alakban, amiből következik, hogy a 2 átkódoló érti a címkét, vagy mert a 2 átkódoló már rendelkezik a hozzáférhető, megfelelő átfordítási eljárással, vagy úgy tervezték, hogy megértse közvetlenül a címkéket, vagy biztosítva van vagy volt számára a 17 eljárásinformáció 1 küldő vagy egy másik forrás által. Abban az esetben, amikor az eljáráscímke-verzió nemkívánatos vagy nem felismerhető valamely oknál fogva, a nem címkézett 12 biztonsági információt és a nem címkézett 13 átkódolásimód-információt továbbítjuk a 2 átkódolóhoz úgy, hogy a 2 átkódolónak nincsen szüksége eljárásinformációra a kapott 12 biztonsági információ és 13 átkó-

dolásimód-információ szerinti átkódolás közvetlen végrehajtásához.

Miután elkészültünk a címkézéssel a D tartalom számára, az 1 küldő képes a D tartalom ábrázolására úgy mint

$$sum(D)=<L(f_1),L(f_2)...L(f_N)> \quad (6)$$

amelyet itt D tartalomösszegzésének, másképpen 11 biztonsági és átkódolásimód-információcsomagnak nevezünk, sum(D)-vel jelölve. A címkéket így összerakjuk a sum(D) tartalomösszegzésben, amely funkciót itt egy 23 csomagosító (packetizer) végez. Az 1 küldő aláírja sum(D)-t sign(sum(D))ként, így 10 aláírást állít elő, melyet az ábrán SIG-gel (SIG – signature) jelölünk, 22 aláírás-generátor használatával a D tartalomban lévő adat összegzésének egy ellenőrizhető módú jelöléseként. A D tartalomösszegzését írjuk alá, nem magát a D tartalmat, mivel a (2) és (3) formulákban lévő címkézési sémák nem tartalmazzák egyik mező aktuális adatait sem. A sum(D) tartalomösszegzés a tartalom egy darabját tartalmazó adat ábrázolásának egy kompakt módja, amely ellenőrizhető a sign(sum(D)) aláírás ellenőrzésével.

A csomagosítófunkciót és a címkézőfunkciót akár össze is vonhatjuk.

A 11 biztonsági és átkódolásimód-információcsomagot továbbítjuk a 2 átkódolóhoz. A kódolt titkos 14 információadatot is és a nem titkos 15 információadatot is továbbítjuk a 2 átkódolóhoz. Más szavakkal a 9 információadatot egy felosztott és részben kódolt formában küldjük át a 2 átkódolóhoz.

Ahhoz, hogy megmagyarázzuk, mennyire biztonságos és ellenőrizhető átkódolást hajtunk végre, tekintsünk egy elrendezést, amelyben a 3 fogadó és az 1 küldő felépítettek egy biztonságos kapcsolatot (session) egy K kódolási kulcs alatti elejétől végéig kódoláshoz. A 3 fogadó által megkapott D tartalmat át kell szűrnünk egy T átkódolószolgáltatáson.

A kért D tartalom minden egyes darabjához az 1 küldő egyezteti a sum(D) tartalomösszegzést, és minden egyes $f_i$ mezőre megvizsgálja annak $L(f_i)$ mezőcímkesorát (tuple), amelyet a sum(D) tartalomösszegzésben talál. Ha a D tartalom tartalmaz biztonságérzékeny információt, akkor a mezők közül néhány vagy potenciálisan valamennyi biztonsági címkéje „biztonságos" lesz.

Az általánosság megsértése nélkül feltehetjük, hogy az első j darab $f_1$, $f_2...f_j$ mező biztonságosnak van címkézve, míg a maradék $f_{j+1}$, $f_{j+2}...f_N$ nem biztonságosnak vannak jelölve. Az 1 küldő ekkor a következő sort (tuple) továbbítja 2 átkódolónak:

$$<sum(D),sign(sum(D)),E_K(d(f_1))... \\ ...E_K(d(f_j)),d(f_{j+1})...d(f_N)> \quad (7)$$

ahol $d(f_i)$ az $f_i$ mezőnek megfeleltetett adat, és $E_K(d(f_i))$ az $f_i$ mezőnek megfeleltetett adat kódolása a K kódolási kulcs alatt. Minden egyes biztonságos mező adatát egyedenként kódoljuk.

A 2 átkódoló tartalmaz TC-vel jelölt 4 döntési eszközt annak eldöntésére, hogy a megkapott, részben kódolt 14, 15 információadat mely részét kell átkódolni 3 fogadóhoz való továbbítás előtt.

Ezáltal a kódolt titkos 14 információadat csak a tartalmának felhasználása nélkül kódolható át, míg a nem titkos 15 információadat átkódolható, lévén hozzáférésünk annak tartalmához.

Elméletben az átkódolás azt jelenti, hogy a megkapott kódolt titkos 14 információadat méretét vagy komplexitását csökkentjük. Ezt megtehetjük változatos szinteken, mint egy nagyon erős átkódolás, mely a kódolt titkos 14 információadat és a nem titkos 15 információadat teljes mértékben minimalizált változatát engedélyezi, és ezzel ellentétesen egy inkább gyenge átkódolás, mely a kódolt titkos 14 információadatot és a nem titkos 15 információadatot csak valamilyen kismértékben csökkenti. Átkódolás tartalmazhat adattömörítést vagy részleges adattörlést. Ehhez a 12 biztonsági információt és a 13 átkódolásimód-információt kiolvassuk a 11 biztonsági és átkódolásimód-információcsomagból, és felhasználjuk a kódolt titkos 14 információadat és a nem titkos 15 információadat átkódolásához, mely így TECD-vel jelölt (TECD – transcoded encrypted confidential data) átkódolt kódolt titkos 24 információadatot és TNCD-vel jelölt (TNCD – transcoded nonconfidential data) átkódolt nem titkos 25 információadatot eredményezi.

A 2 átkódoló itt két lépésben működik a megkapott részben kódolt 14, 15 információadat-folyamon. Az első lépésben az átkódoló sorosítja az adatot az almezőstruktúra eltávolításával minden egyes mezőről. Például, ha $f_i$ egy mező, és $f_{i,j}$ almezője $f_i$-nek, ez a sorosítás elképzelhető úgy, mint a következő művelet végrehajtása:

$$d(f_i)=<.,d(f_{i,j}),.>---> <.<ptr>,.>, ptr:<d(f_{i,j})>. \quad (8)$$

A sorosítás úgy működik, hogy az almezőadatot egy odamutató pointerrel helyettesítjük, ahol az almezőadat található az adatfolyamban. Ez a hierarchikus adatstruktúra egy egyenes, egymásba ágyazásoktól mentesített ábrázoláshoz vezet.

A második lépésben a 2 átkódoló megvizsgálja a nem biztonságos $f_{j+1}$, $f_{j+2}...f_N$ mezőket és végrehajt valamely megfelelő átkódolást, amelynek kimenetét $T(f_{j+1}, f_{j+2}...f_N)$ jelöli. Bármely nem kritikus $f_i$ mezőre, amelyet eltávolítunk a végső adatfolyamból az átkódolás után, az átkódoló megvizsgálja $d(f_i)$-t is. Ha $d(f_i)$ tartalmaz mutatót almezőadatra, ezt az adatot is eltávolítjuk. Ha egy átkódolható eltávolítandó mező tartalmaz biztonságos kódolt almezőt, akkor az almezőadat eltávolítása megváltoztatja $E_K(d(f_1))...E_K(d(f_j))$-t úgy, hogy $T(E_K(d(f_1))...E_K(d(f_j)))$ jelöli a kódolt mezők listáját, miután az átkódolás következtében bármilyen törlést végeztünk.

Végül a 2 átkódoló továbbítja a következő 4 hosszú sort (4-tuple) a kérelmező 3 fogadónak:

$$<sum(D),sign(sum(D)),T(E_K(d(f_1))... \\ ...E_K(d(f_j))),T(d(f_{j+1})...d(f_N))> \quad (9)$$

A 3 fogadó tartalmaz egy 6 integritás-ellenőrző eszközt, mely a 10 aláíráson végez műveletet, és 19 integritás-ellenőrző kimenetként szolgáltat egy integritás-ellenőrző információt, amely jelzi, hogy a 11 biztonsági és átkódolásimód-információcsomag megváltozott-e tartalmában az 1 küldő és a 3 fogadó között, vagy sem.

A 3 fogadó továbbá tartalmaz egy 8 eljárásinformáció-értelmezőt, mely segít a 17 eljárásinformáció használatakor a 13 átkódolásimód-információcímkék és a 12 biztonságiinformáció-címkék értelmezésében. Erre a 8 eljárásinformáció-értelmezőre nincsen szükség, ha a 3 fogadó már megérti a címkenyelvet. Másrészről egy ilyen 8 eljárásinformáció-értelmező a 2 átkódolóban is használható, ha az nem érti meg a címkenyelvet, de felhasználja a 17 eljárásinformációt.

Az értelmezett címkéket ezután egy 7 összehasonlító eszköz használja annak eldöntésére, hogy az átkódolt kódolt titkos 24 információadat és az átkódolt nem titkos 25 információadat a címkékben lévő szabályok szerint lettek-e átkódolva és kezelve. Az eredmény egy 27 indikátorkimenet arra nézve, hogy a kapott átkódolt 24, 25 információadat megbízható-e vagy sem. Végül az átkódolt kódolt titkos 24 információadatot 26 dekódolóval dekódoljuk, mely 18 dekódolókimenetként adja a dekódolt titkos információadatot. Az átkódolt nem titkos 25 információadat nem igényel további műveletet és 20 átkódolt nem titkos információadat kimeneteként közvetlenül adódik.

Az eredeti, 1 küldőn létező D tartalom struktúráját sum(D)-ben ábrázoljuk, melyet 3 fogadó ellenőrizhet a szerver sign(sum(D)) aláírásának ellenőrzésével sum(D)-n. Így 3 fogadó képes a D tartalmat ábrázoló mezők halmazának meghatározására, ahogyan azt 1 küldő specifikálta. Továbbá, mivel sum(D) biztonsági és átkódolásimód-információcsomag tartalmaz D tartalom minden egyes mezőjéhez címkesorokat (tuples), a 3 fogadó ellenőrizheti a címkézést, amit 1 küldő választott a D tartalommezőihez. Különösen, a 3 fogadó meghatározhatja, hogy az 1 küldő melyik mezőket jelölte meg biztonságosként, és hogy az 1 küldő melyeket jelölt meg átkódolhatóként.

Ezután a 3 fogadó ellenőrzi, hogy az összes mezőt, amelyeket a sum(D) biztonsági és átkódolásimód-információcsomagban biztonságosként és kritikusként specifikáltunk, a 2 átkódoló nem törölte vagy módosította a $T(E_K(d(f_1))...E_K(d(f_j)))$ átkódolt kódolt információadatban. Itt ezen ellenőrzés legalábbis egy részét az E kódolási algoritmus biztosítja, mely tartalmazhat eredetiségi információt a kódolásra került adatokról.

Továbbá a 3 fogadó összehasonlítja a sum(D)-ben meghatározott átkódolható mezők halmazát a megkapott $T(d(f_{j+1})...d(f_N))$ mezőkkel annak ellenőrzésére, hogy az átkódolási folyamat nem törölt vagy nem megfelelően módosított bármely tartalmat, amely a 3 fogadónál ábrázolható lenne.

## SZABADALMI IGÉNYPONTOK

1. Eljárás információadat (9) továbbítására küldőtől (1) fogadóhoz (3) átkódolón (2) keresztül, ahol az információadat (9) titkos információadatot (16) és nem titkos információadatot (15) tartalmaz, *azzal jellemezve,* hogy a titkos információadatot (16) kódolt titkos információadat (14) formára kódoljuk, amely a nem titkos információadattal (15) együtt képezi a részben kódolt információadatot (14, 15), és a részben kódolt információadattal (14, 15) együtt biztonsági információt (12) és átkódolásimód-információt (13) küldünk el az átkódolónak (2), a biztonsági információt (12) és az átkódolásimód-információt (13) az átkódolóval (2) egy átkódolási lépésben felhasználjuk, amelynek során a kódolt titkos információadat (14) tartalmához nem férünk hozzá, míg a nem titkos információadat (15) tartalmához az átkódolásnál hozzáférünk, tehát az átkódolóval (2) az átkódolási lépésben eldöntjük, hogy a részben kódolt információadat (14, 15) mely részét továbbítjuk a fogadóhoz (3) és/vagy változtatjuk meg a továbbítás előtt.

2. Az 1. igénypont szerinti eljárás, *azzal jellemezve,* hogy a részben kódolt információadathoz (14, 15) ellenőrző (hashing) információt társíthatunk megengedve a tartalom ellenőrzését a fogadónál (3) a részben kódolt információadat (14, 15) legalább egy részénél.

3. Az 1. vagy 2. igénypont szerinti eljárás, *azzal jellemezve,* hogy az információadatot (9) információadatdarabokra bontjuk fel a kódolás és továbbítás előtt.

4. A 3. igénypont szerinti eljárás, *azzal jellemezve,* hogy minden egyes információadat-darabhoz hozzárendeljük a saját darab biztonságiinformáció-részét és darab kódolásimód-információrészét.

5. Az 1–4. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy az információadat-darabok legalább egyikéhez hozzárendeljük a saját darab ellenőrző- (hashing) információ-részt, ahol az információadat-darab előnyösen a nem titkos információadat (15) részét képezi.

6. A 4. vagy 5. igénypont szerinti eljárás, *azzal jellemezve,* hogy a darab biztonságiinformáció-részeket és a darab átkódolásimód-információrészeket címkékre (SIL, TIL) fordítjuk át átfordítási eljárás szerint, és a darab biztonságiinformáció-részek és darab átkódolásimód-információrészek helyett a címkéket (SIL, TIL) továbbítjuk az átkódolóhoz (2), továbbá az eljárásinformációt (17), amely megadja, hogy a címkéket (SIL, TIL) hogyan kell értelmezni, elérhetővé tesszük vagy már elérhető az átkódoló (2) számára.

7. A 6. igénypont szerinti eljárás, *azzal jellemezve,* hogy a címkéket (SIL, TIL) biztonsági és átkódolásimód-információcsomagban (11) kombináljuk, amelyet a fogadónál (3) tartalomintegritás-ellenőrzést lehetővé tévő aláírással (10) egészítünk ki.

8. Eljárás részben kódolt információadat (14, 15) átkódolására átkódolóban (2), melyet küldőtől (1) kapunk meg, és fogadóhoz (3) kell továbbítanunk, *azzal jellemezve,* hogy a részben kódolt információadat (14, 15) tartalmaz nem titkos információadatot (15) és kódolt titkos információadatot (14), és amelyhez biztonsági információt (12) és átkódolásimód-információt (13) társítunk, melyet annak eldöntésére használunk, hogy a részben kódolt információadat (14, 15) mely részét kell átkódolnunk a fogadóhoz (3) történő továbbítás előtt, ahol a kódolt titkos információadatot (14) csak tartalmának felhasználása nélkül kódoljuk át, míg a nem titkos információadatot (15) a tartalom hozzáférésével kódoljuk át.

9. A 8. igénypont szerinti eljárás, *azzal jellemezve,* hogy a részben kódolt információadatot (14, 15) információadat-darabokra felosztva fogadjuk.

10. A 9. igénypont szerinti eljárás, *azzal jellemezve,* hogy minden egyes információadat-darabhoz hozzárendeljük saját darab biztonságiinformáció-részét és darab átkódolásimód-információrészét.

11. A 10. igénypont szerinti eljárás, *azzal jellemezve,* hogy a darab biztonságiinformáció-részeket és a darab átkódolásimód-információrészeket címkék (SIL, TIL) formájában kapjuk meg, és az átkódoláshoz az átkódoló (2) számára elérhető eljárásinformációt (17) használunk, amellyel megmondjuk, hogy hogyan értelmezzük a címkéket (SIL, TIL).

12. A 11. igénypont szerinti eljárás, *azzal jellemezve,* hogy a címkéket (SIL, TIL) biztonsági és átkódolásimód-információcsomagban (11) kombinálva fogadjuk, és a csomagot a fogadónál (3) tartalomintegritás-ellenőrzést lehetővé tévő aláírással (10) egészítjük ki.

13. Eljárás átkódolt nem titkos információadatot (25) és átkódolt kódolt titkos információadatot (24) tartalmazó átkódolt részben kódolt információadat (24, 25) fogadására fogadónál (3) átkódolótól (2), *azzal jellemezve,* hogy az átkódolt részben kódolt információadattal (24, 25) együtt biztonsági információt (12) és átkódolásimód-információt (13) fogadunk, amelyeket az átkódolt részben kódolt információadattal (24, 25) való összehasonlításhoz használunk, az átkódolásnak a biztonsági információhoz (12) és átkódolásimód-információhoz (13) való megfelelésének tesztelésére.

14. A 13. igénypont szerinti eljárás, *azzal jellemezve,* hogy a részben kódolt információadathoz (14, 15) ellenőrző (hashing) információt társítunk a tartalom ellenőrzésére a fogadónál (3) az átkódolt részben kódolt információadat (24, 25) legalább egy részénél.

15. A 13. vagy 14. igénypont szerinti eljárás, *azzal jellemezve,* hogy az átkódolt részben kódolt információadatot (24, 25) információadat-darabokra osztva fogadjuk.

16. A 13–15. igénypontok bármelyike szerinti eljárás, *azzal jellemezve,* hogy az információadat-darabok legalább egyikéhez hozzárendeljük a saját darab ellenőrző- (hashing) információ-részét, mely információadat-darab célszerűen része a nem titkos információadatnak (15).

17. A 15. vagy 16. igénypont szerinti eljárás, *azzal jellemezve,* hogy a darab biztonságiinformáció-részeket és darab átkódolásimód-információrészeket címkék (SIL, TIL) formájában fogadjuk, továbbá a fogadó (3) számára elérhető eljárásinformációt (17) a címkék (SIL, TIL) értelmezésére használjuk, és ezáltal az átkódolás helyességét teszteljük.

18. A 17. igénypont szerinti eljárás, *azzal jellemezve,* hogy a címkéket (SIL, TIL) tartalmazó biztonsági és átkódolásimód-információcsomag (11) tartalomintegritás-ellenőrzését aláírás (10) használatával hajtjuk végre.

19. Küldő (1) információadat (9) továbbítására fogadónak (3) átkódolón (2) keresztül, amely az információadatot (9) átkódolja a fogadóhoz (3) való továbbítás előtt, ahol az információadat (9) tartalmaz titkos információadatot (16) és nem titkos információadatot (15), *azzal jellemezve,* hogy a küldő (1) tartalmaz kódolót (5) a titkos információadat (16) kódolására, előállító eszközt biztonsági információ (12) és átkódolásimód-információ (13) előállítására, valamint csatolóeszközt, amely a biztonsági információt (12) és az átkódolásimód-információt (13) a részben kódolt információadathoz (14, 15) csatolja az átkódolónak való továbbítás előtt, ahol a biztonsági információ (12) és átkódolásimód-információ (13) megakadályozza a hozzáférést a titkos adatokhoz, és lehetővé teszi a hozzáférést a nem titkos adatokhoz az átkódolás során.

20. A 19. igénypont szerinti küldő (1), *azzal jellemezve,* hogy tartalmaz darabolóeszközt (21) az információadat (9) kódolás és továbbítás előtti felosztására információadat-darabokra.

21. A 20. igénypont szerinti küldő (1), *azzal jellemezve,* hogy minden egyes információadat-darabhoz saját darab biztonságiinformáció-rész és darab átkódolásimód-információrész tartozik, és a küldő (1) tartalmaz átfordítóeszközt a darab biztonságiinformáció-részek és a darab átkódolásimód-információrészek címkékre (SIL, TIL) történő átfordítására, amelyek továbbíthatók az átkódolóhoz (2), továbbá átfordításieljárás-információtárolót átfordításieljárás-információ (17) tárolására és az átkódolóhoz (2) továbbításra vagy elérhetővé tételre, ahol az eljárásinformáció (17) megadja, hogy a címkéket (SIL, TIL) hogyan kell értelmezni.

22. A 21. igénypont szerinti küldő (1), *azzal jellemezve,* hogy tartalmaz csomagosítót (23), amely a címkéket (SIL, TIL) biztonsági és átkódolásimód-információcsomagban (11) kombinálja, és aláírásgenerátort (22), amely a csomagot (11) a fogadónál (3) tartalomintegritás-ellenőrzést lehetővé tévő aláírással (10) látja el.

23. Átkódoló (2) küldőtől (1) fogadott részben kódolt információadat (14, 15) átkódolására és az átkódolt részben kódolt információadat (24, 25) fogadóhoz (3) való továbbítására, ahol a fogadott részben kódolt információadat (14, 15) tartalmaz nem titkos információadatot (15) és kódolt titkos információadatot (14), és amelyhez biztonsági információ (12) és átkódolásimód-információ (13) van társítva, *azzal jellemezve,* hogy az átkódoló (2) tartalmaz döntési eszközt (4) annak eldöntésére, hogy a fogadott részben kódolt információadat (14, 15) mely részét kell átkódolni a fogadóhoz (3) való továbbítása előtt, ahol a kódolt titkos információadat (14) csak a tartalmának felhasználása nélkül kódolható át, míg a nem titkos információadat (15) átkódolható annak tartalmához való hozzáféréssel is.

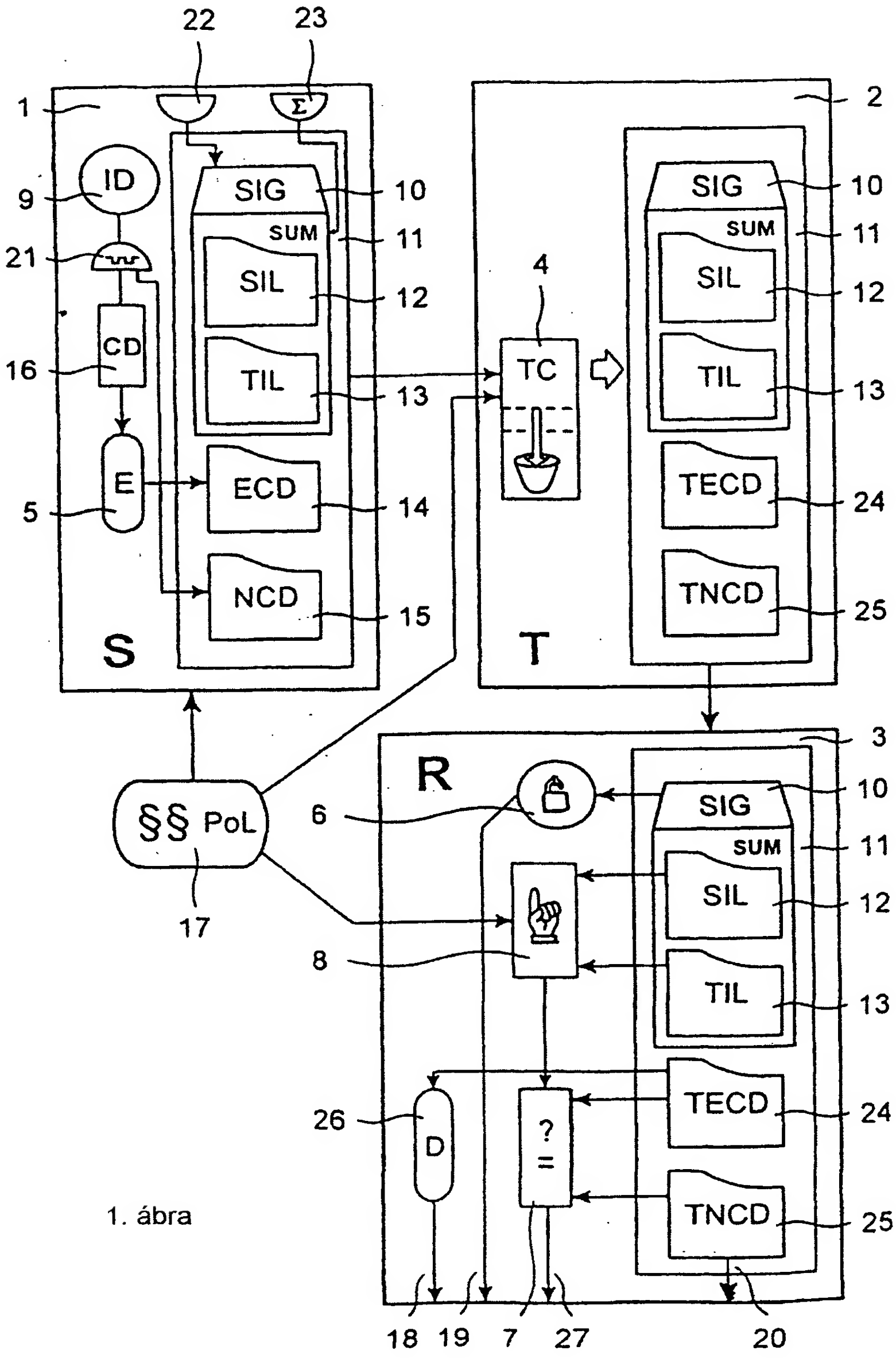
24. A 23. igénypont szerinti átkódoló (2), *azzal jellemezve,* hogy tartalmaz vevőeszközt az információadat darabokra osztott részben kódolt információadat (14, 15) vételére, ahol minden egyes információadat-darabhoz saját darab biztonságiinformáció-rész és darab átkódolásimód-információrész tartozik, előnyösen címkék (SIL, TIL) formájában, valamint eljárás információtároló- vagy -vevő eszközt az eljárásinformáció tárolására vagy vételére, ahol az eljárásinformáció (17) az

átkódoláshoz megadja, hogy hogyan kell értelmezni a címkéket (SIL, TIL).

25. Fogadó (3) átkódolt részben kódolt információadat (24, 25) fogadására küldőtől (1) átkódolón (2) keresztül, amely átkódolt részben kódolt információadat (24, 25) tartalmaz átkódolt nem titkos információadatot (25) és átkódolt kódolt titkos információadatot (24), továbbá az átkódolt részben kódolt információadattal (24, 25) együtt biztonsági információ (12) és átkódolásimód-információ (13) fogadására, *azzal jellemezve,* hogy tartalmaz összehasonlító eszközt (7) a biztonsági információnak (12) és az átkódolásimód-információnak (13) az átkódolt részben kódolt információadathoz (24, 25) való hasonlítására az átkódolásnak a biztonsági információhoz (12) és átkódolásimód-információhoz (13) való megfelelésének tesztelésére.

26. A 25. igénypont szerinti fogadó (3), *azzal jellemezve,* hogy az átkódolt részben kódolt információadat (24, 25) információadat-darabokból áll, a darab biztonságiinformáció-részeket és darab átkódolásimód-információrészeket címkék (SIL, TIL) helyettesítik, és az eljárásinformációt (17) is használó összehasonlító eszközhöz (7) eljárásinformáció-értelmező (8) tartozik, amely lehetővé teszi a címkék (SIL, TIL) értelmezését, és így az átkódolás helyességének tesztelését.

27. A 26. igénypont szerinti fogadó (3), *azzal jellemezve,* hogy integritás-ellenőrző eszköze (6) is van a címkéket (SIL, TIL) tartalmazó biztonsági és átkódolásimód-információcsomag (11) tartalomintegritás-ellenőrzésére a biztonsági és átkódolásimód-információcsomag (11) aláírásának (10) használatával.




1. ábra

Kiadja a Magyar Szabadalmi Hivatal, Budapest
A kiadásért felel: Törőcsik Zsuzsanna főosztályvezető-helyettes
Windor Bt., Budapest